CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, via EFS-Web, on August 24, 2010.

/Wesley L. Austin/

Attorney for Applicants

PATENT APPLICATION
Docket No. AUZ-002 P

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	David M. Austin et al.	
Serial No.:	10/027,714	
Filed:	December 21, 2001	Group Art Unit: 2134
For:	DETECTION OF OBSERVERS AND COUNTERMEASURES AGAINST OBSERVERS	
Examiner:	Thomas M. Szymanski	

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

An Office Action dated December 24, 2009 (hereinafter, "Office Action") rejected all pending claims (claims 1-21) in the present application. A Notice of Appeal was submitted on June 24, 2010. Appellant's Appeal Brief is being filed herewith.

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest is the assignee, Trapware Corporation.

2. RELATED APPEALS AND INTERFERENCES

An appeal had been filed in the parent patent application, Application No. 09/491,727. A Notice of Appeal was filed on June 6, 2005. In response to the Notice of Appeal and Appeal Brief, the finality of the last office action on App. No. 09/491,727 was withdrawn and a new office action was mailed on April 21, 2006. An appeal had been filed in this patent application, Application No. 10/027,714 on July 10, 2006. The Board of Patent Appeals and Interferences decided the appeal on July 28, 2008.

3. STATUS OF CLAIMS

Claims 1-21 are pending in the present application. Claims 22-34 have been withdrawn from consideration due to a restriction/election requirement. Claims 1-21 have been rejected under 35 U.S.C. § 103(a) based on Togawa, U.S. Patent No. 6,240,530 (hereinafter, "Togawa"), in view of Drake, U.S. Patent No. 6,006,328 (hereinafter, "Drake") and in further view of Kim, U.S. Patent No. 6,701,440 (hereinafter, "Kim").

Appellants appeal the rejections of claims 1-21.

4. STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

As stated in the background section of the patent application, software has been developed to observe or monitor computer users. These software programs provide a wide variety of monitoring features. For example, some of these programs are able to log keystrokes of a user, log menu commands, take screen shots of a user's computer screen at various times, track use of various programs, track what web sites have been visited, monitor e-mail communications, etc. With the technology available today, most, if not all, of a computer user's activities on a computer can be observed and recorded. See the Appellants' patent application (hereinafter referred to as the

"Specification"), page 2, lines 24-31; page 3, lines 1-13.

With the computer technology of today and with the observing programs now available and for those programs that will surely be developed and used in the future, computer users may be watched by third parties more often than many think. It would be highly beneficial to computer users if they could find out whether they are being observed by computer software and technology and to know information about the observing activity and/or program. Specification, page 2, lines 24-31; page 3, lines 1-13.

As required by 37 C.F.R. § 41.37(c)(1)(v), a summary of claimed subject matter immediately follows. The references to the specification refer only to embodiments of the invention. The invention is defined by the claims. Accordingly, these references to the specification are not meant to limit the scope of the claims of the present invention in any way but are only provided because they are mandated by 37 C.F.R. § 41.37(c)(1)(v). All references are to the patent specification.

1. A computer program embodied in a computer-readable medium for scanning a computer for observer programs, the computer program comprising:

observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data, and wherein the log data includes screen shots, program usage and web sites visited; (pg. 7, lines 20-22; pg. 8, lines 9-20; pg. 11, lines 8-31; pg. 12, lines 1-31; pg. 13, lines 1-12; Figure 2, elements 34-48; pg. 14, lines 19-31; pg. 15, lines 1-31; pg. 16, lines 1-25)

reading instructions that read memory of the computer to obtain memory data; (pg. 7, lines 22-24; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 9, lines 5-14; pg. 13, lines 13-31; pg. 14, lines 1-31; pg. 15, lines 1-31; pg. 16, lines 1-25; Figure 3, elements 50-60; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer; (pg. 7, lines 24-26; pg. 7, lines 29-31; pg. 8, lines 1-5; pg. 8, lines 21-

31; pg. 9, lines 1-4; pg. 13, lines 28-31; pg. 14, lines 1-31; pg. 15, lines 1-31; pg. 16, lines 1-25; Figure 3, elements 50-60; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

generating instructions that generate results from the comparing, wherein the results generated indicate whether the observer program is present on the computer; (pg. 7, lines 26-29; pg. 7, lines 29-31; pg. 8, lines 1-5; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 16, lines 26-31; Figure 4; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

countermeasure instructions that alter the operation of the observer program; and (pg. 17, lines 1-10; pg. 21, lines 29-31; pg. 22, lines 1-5; Figure 4; Figure 7; Figure 8; Figure 9)

outputting instructions that provide the results through a graphical user interface and that prompt as to whether the countermeasure instructions should be executed. (pg. 8, lines 6-8; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 16, lines 26-31; Figure 4; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

21. A method embodied in a computer-readable medium for scanning a computer for observer programs, the method comprising:

using observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data, and wherein the log data includes screen shots, program usage and web sites visited; (pg. 7, lines 20-22; pg. 8, lines 9-20; pg. 11, lines 8-31; pg. 12, lines 1-31; pg. 13, lines 1-12; Figure 2, elements 34-48; pg. 14, lines 19-31; pg. 15, lines 1-31; pg. 16, lines 1-25)

reading memory of the computer to obtain memory data; (pg. 7, lines 22-24; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 9, lines 5-14; pg. 13, lines 13-31; pg. 14, lines 1-31; pg. 15, lines 1-31; pg. 16, lines 1-25; Figure 3, elements 50-60; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

comparing the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer; (pg. 7, lines 24-26; pg. 7, lines 29-31; pg. 8, lines 1-5; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 13, lines 28-31; pg. 14, lines 1-31; pg. 15, lines 1-31; pg. 16, lines 1-25; Figure 3, elements 50-60; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

generating results from the comparing, wherein the results generated indicate whether the observer program is present on the computer (pg. 7, lines 26-29; pg. 7, lines 29-31; pg. 8, lines 1-5; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 16, lines 26-31; Figure 4; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

outputting the results through a graphical user interface; and (pg. 8, lines 6-8; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 16, lines 26-31; Figure 4; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

prompting the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running. (pg. 17, lines 1-10; pg. 21, lines 29-31; pg. 22, lines 1-5; Figure 4; Figure 7; Figure 8; Figure 9)

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following issues are presented for review:

A. Whether claims 1-21 are unpatentable under 35 U.S.C. § 103(a) based on Togawa in view of Drake in view of Kim.

7. ARGUMENT

A. Claims 1-21 Rejected Under 35 U.S.C. § 103(a)

The Examiner rejected claims 1-21 under 35 U.S.C. § 103(a) based on Togawa, U.S. Patent No. 6,240,530 (hereinafter, "Togawa"), in view of Drake, U.S. Patent No. 6,006,328 (hereinafter, "Drake") and in further view of Kim, U.S. Patent No. 6,701,440 (hereinafter, "Kim"). This rejection is respectfully traversed.

The M.P.E.P. states that

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure.
>
> The initial burden is on the examiner to provide some suggestion of the desirability of doing what the inventor has done. To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references.

M.P.E.P. § 2142.

Appellants respectfully submit that the claims at issue are patentably distinct from the cited references.

Rejection of Claims 1-20

Togawa does not teach or suggest "countermeasure instructions that alter the operation of the observer program; and outputting instructions . . . that prompt as to whether the countermeasure instructions should be executed."

Towaga, alone or in combination with Drake, does not teach or suggest this subject matter. Instead Towaga states:

> According to a further aspect of the present invention, there is provided an information processing apparatus which includes a memory for storing programs and data for information processing and a processing section for executing the

> programs to perform various information processing, comprising a virus detection and identification section for detecting a computer virus which infects the information processing apparatus and identifying a type of the detected computer virus, a virus type information registration section for registering information regarding the type of the detected computer virus identified by the virus detection and identification section into a storage area which is access-disabled in an ordinary operation of the information processing apparatus, a trigger information outputting section for outputting trigger information so that the information processing apparatus may enter a processing mode for performing virus extermination, a stored information clearing section operable in response to the trigger information from the trigger information outputting section for clearing information stored in all of those areas of the memory which are access-enabled in an ordinary operation of the information processing apparatus, an operating system fetching and starting up section for fetching an operating system from the outside and starting up the operating system after the stored information is cleared by the stored information clearing section, and a virus extermination section for exterminating, in operation environment of the operating system started up by the operating system fetching and starting up section, the computer virus which infects the memory of the information processing apparatus based on the information regarding the type of the detected virus registered in the virus type information storage section.

Togawa, col. 5, lines 7-38. This portion of Togawa does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

Togawa also states:

> FIG. 1 illustrates in flow chart a virus extermination method according to an aspect of the present invention. Referring to FIG. 1. the virus extermination method illustrated includes a virus detection and identification step S1, a memory clearing step S3, an operating system fetching and starting up step S4 and a virus extermination step S5 in order to exterminate a computer virus as a software destroying factor which infects a computer system.
>
> More particularly, in the virus detection and identification step S1, a computer virus as a software destroying factor which infects a computer system is detected and a type of the computer virus is identified. If such an infecting computer virus is detected in the virus detection and identification step S1 (the YES route of step S2), then information stored in all of those areas of a memory which are in a write-enabled state in an ordinary operation of the computer system is cleared in the memory clearing step S3.

Togawa, col. 8, lines 14-30. This portion of Togawa does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

The addition of Drake does not overcome the deficiencies of Togawa. Instead Drake states:

> The improved process consists of including computer code to automatically detect tampering of said computer software, and computer code to prevent the theft of ID-Data by replacing existing vulnerable (to rogue software eavesdropping or attack) software or operating system code with secure equivalents which utilise anti-spy techniques (as described later in this document).

Drake, col. 3, lines 38-44. This portion of Drake does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

Drake also states:

> This can be achieved with the use of code which is protected from disassembly and examination through obfuscation and encryption, which re-reads its own external-image and compares it with its known memory image or precalculated check-data to detect hot-patching (ie. the modification of software sometime after it has been loaded from disk, but (usually) before execution of the modified section has commenced).
>
> Additionally, the software can scan the memory image of itself one or more times, or continuously, to ensure that unexpected alterations do not occur.

Drake, col. 6, lines 10-20. This portion of Drake does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

Claim 1 also recites "outputting instructions . . . that prompt as to whether the countermeasure instructions should be executed." Towaga, alone or in combination with Drake, does not teach or suggest this subject matter. Instead Togawa states:

> According to a further aspect of the present invention, there is provided an information processing apparatus which includes a memory for storing programs and data for information processing and a processing section for executing the programs to perform various information processing, comprising a virus detection and identification section for detecting a computer virus which infects the information processing apparatus and identifying a type of the detected computer virus, a virus type information registration section for registering information regarding the type of the detected computer virus identified by the virus detection and identification section into a storage area which is access-disabled in an ordinary operation of the information processing apparatus, a trigger information outputting section for outputting trigger information so that the information processing apparatus may enter a processing mode for performing virus extermination, a stored information clearing section operable in response to the trigger information from the trigger information outputting section for clearing information stored in all of those areas of the memory which are access-enabled in an ordinary operation of the information processing apparatus, an operating system fetching and starting up section for fetching an operating system from the outside and starting up the operating system after the stored information is cleared by the stored information clearing section, and a virus extermination section for

> exterminating, in operation environment of the operating system started up by the operating system fetching and starting up section, the computer virus which infects the memory of the information processing apparatus based on the information regarding the type of the detected virus registered in the virus type information storage section.

Togawa, col. 5, lines 7-38. This portion of Togawa does not teach or suggest "outputting instructions that provide the results through a graphical user interface and that prompt as to whether the countermeasure instructions should be executed."

Togawa also states:

> FIG. 1 illustrates in flow chart a virus extermination method according to an aspect of the present invention. Referring to FIG. 1. the virus extermination method illustrated includes a virus detection and identification step S1, a memory clearing step S3, an operating system fetching and starting up step S4 and a virus extermination step S5 in order to exterminate a computer virus as a software destroying factor which infects a computer system.
>
> More particularly, in the virus detection and identification step S1, a computer virus as a software destroying factor which infects a computer system is detected and a type of the computer virus is identified. If such an infecting computer virus is detected in the virus detection and identification step S1 (the YES route of step S2), then information stored in all of those areas of a memory which are in a write-enabled state in an ordinary operation of the computer system is cleared in the memory clearing step S3.

Togawa, col. 8, lines 14-30. This portion of Togawa does not teach or suggest "outputting instructions that provide the results through a graphical user interface and that prompt as to whether the countermeasure instructions should be executed."

The addition of Drake does not overcome the deficiencies of Togawa. Instead Drake states:

> The improved process consists of including computer code to automatically detect tampering of said computer software, and computer code to prevent the theft of ID-Data by replacing existing vulnerable (to rogue software eavesdropping or attack) software or operating system code with secure equivalents which utilise anti-spy techniques (as described later in this document).

Drake, col. 3, lines 38-44. This portion of Drake does not teach or suggest "outputting instructions that provide the results through a graphical user interface and that prompt as to whether the countermeasure instructions should be executed."

Drake also states:

> This can be achieved with the use of code which is protected from disassembly and examination through obfuscation and encryption, which re-reads its own external-image and compares it with its known memory image or precalculated check-data to detect hot-patching (ie. the modification of software sometime after it has been loaded from disk, but (usually) before execution of the modified section has commenced).
>
> Additionally, the software can scan the memory image of itself one or more times, or continuously, to ensure that unexpected alterations do not occur.

Drake, col. 6, lines 10-20. This portion of Drake does not teach or suggest "outputting instructions that provide the results through a graphical user interface and that prompt as to whether the countermeasure instructions should be executed."

Kim also does not teach or suggest "countermeasure instructions that alter the operation of the observer program; and outputting instructions . . . that prompt as to whether the countermeasure instructions should be executed." Kim only teaches a system for protecting a computer using a remote e-mail scanning device. (Kim , Abstract.)

In view of the foregoing, Applicants respectfully submit that claim 1 is patentably distinct from the cited references. Accordingly, Applicants respectfully request that the rejection of claim 1 be withdrawn because Towaga, alone or in combination with Drake and Kim, does not teach or suggest all of the subject matter of claim 1.

As set forth above, neither Togawa, Drake nor Kim teach or suggest all of the limitations in claim 1. Claims 2-20 depend directly or indirectly from claim 1. Thus, Appellants respectfully request that the rejection of claims 2-20 be withdrawn for at least the same reasons.

Rejection of Claims 21

Claim 21 includes similar limitations as claim 1 which were argued above. Thus, Appellants respectfully request that the rejection of claim 21 be withdrawn for at least the same reasons. In addition, claim 21 also requires "prompting the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running." Thus, claim 21 requires that the countermeasure instructions be executable to perform all three actions "(1) temporarily disable the observer program, (2) permanently disable the observer program,

and (3) create decoy observer created data but wherein the observer program continues running." In addition to what was argued above, the cited references further do not teach or suggest countermeasure instructions that are executable to perform these three distinct actions.

None of Towaga, Drake nor Kim teach or suggest countermeasure instructions that are executable to "(3) create decoy observer created data but wherein the observer program continues running." With the present invention, a user is being watched on a computer system and thus, if he or she wanted to create decoy data that would allow him or her to continue using the computer while also maintaining the illusion to the watcher that they were still observing their activities on the computer system. However, with the cited references, there is no reason whatsoever that those pieces of cited prior art would have a reason to "(3) create decoy observer created data but wherein the observer program continues running." Ignoring the fact that this claim limitation is found nowhere in the prior art, the Office Action does not provide "articulated reasoning with some rational underpinning" as to why a person of ordinary skill in the art would try to achieve this with the cited references. (KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 418 (2007) (citing In re Kahn, 441 F.3d 977, 988 (CA Fed. 2006)).)

Respectfully submitted,

/Wesley L. Austin/

Wesley L. Austin
Reg. No. 42,273
Attorney for Appellant(s)

Date: August 24, 2010

AUSTIN RAPP & HARDMAN
170 South Main Street, Suite 735
Salt Lake City, UT 84101
Telephone: (801) 537-1700

CLAIMS APPENDIX

Listing of Claims involved in the appeal:

1. A computer program embodied in a computer-readable medium for scanning a computer for observer programs, the computer program comprising:

observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data, and wherein the log data includes screen shots, program usage and web sites visited;

reading instructions that read memory of the computer to obtain memory data;

comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer;

generating instructions that generate results from the comparing, wherein the results generated indicate whether the observer program is present on the computer;

countermeasure instructions that alter the operation of the observer program; and

outputting instructions that provide the results through a graphical user interface and that prompt as to whether the countermeasure instructions should be executed.

2. The computer program of claim 1 wherein the memory data includes startup commands.

3. The computer program of claim 1 wherein the memory data includes registry startup commands.

4. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer import table data and wherein the comparing instructions compare memory import table data from the memory data characteristics with the observer import table data to determine whether an observer program is present on the computer.

5. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer export table data and wherein the comparing instructions compare memory export table data from the memory data characteristics with the observer export table data to determine whether an observer program is present on the computer.

6. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer resource data and wherein the comparing instructions compare memory resource data from the memory data characteristics with the observer resource data to determine whether an observer program is present on the computer.

7. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer file content data and wherein the comparing instructions compare memory file content data from the memory data characteristics with the observer file content data to determine whether an observer program is present on the computer.

8. The computer program of claim 7 wherein the comparing instructions compare the observer file content data with the memory file content data at an offset address.

9. The computer program of claim 7 wherein the comparing instructions compare the observer file content data with a span of the memory file content identified by an offset address.

10. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer module loading data and wherein the comparing instructions compare memory module loading data from the memory data characteristics with the observer module loading data to determine whether an observer program is present on the computer.

11. The computer program of claim 1 wherein the plurality of observer program characteristics includes OS observing functions and wherein the comparing instructions compare memory functions from the memory data characteristics with the OS observing functions to determine whether an observer program is present on the computer.

12. The computer program of claim 1 wherein the memory data includes explorer extension data.

13. The computer program of claim 1 wherein the memory data includes file use information.

14. The computer program of claim 1 wherein the memory data includes process information.

15. The computer program of claim 1 wherein the memory data includes running process information.

16. The computer program of claim 1 wherein the memory data includes loaded modules information.

17. The computer program of claim 1 wherein the memory data includes driver data.

18. The computer program of claim 1 wherein the memory data includes kernel driver data.

19. The computer program of claim 1 wherein the computer program further comprises disabling instructions to disable the observer program if it is present on the computer, the disabling instructions implementing a method comprising:
entering a startup command to load a kill program before the observer program is started;
rebooting the computer;
starting the kill program by execution of the startup command; and

deleting an observer program startup command so that the observer program is not started.

20. The computer program of claim 19 wherein the method further comprises deleting observer program files.

21. A method embodied in a computer-readable medium for scanning a computer for observer programs, the method comprising:

using observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data, and wherein the log data includes screen shots, program usage and web sites visited;

reading memory of the computer to obtain memory data;

comparing the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer;

generating results from the comparing, wherein the results generated indicate whether the observer program is present on the computer;

outputting the results through a graphical user interface; and

prompting the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running.

22-34. (Withdrawn)

EVIDENCE APPENDIX

NONE.

RELATED PROCEEDINGS APPENDIX

NONE.